UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/523,760	01/30/2006	Joseph E McIsaac	BCIL-0111US	7549

35859 7590 06/28/2010

Pierce Atwood LLP
160 Federal Street
10th Floor
Boston, MA 02110

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
06/28/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

BostonPatent@pierceatwood.com
ceverett@pierceatwood.com

Office Action Summary	Application No.	Applicant(s)	
	10/523,760	MCISAAC ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/31/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to amendment filed 3/31/2010. Claims 1 5-6, 8-17, 20-25, 31, 33, 35, 37-42, 44-46, 48-56, 59-63, 68, 70, 72, 74-82, 84, 86, 88, 90-93 and 95, have been amended. Claims 1-95 are pending.

Specification

2. The disclosure is objected to because it contains an embedded hyperlink (par. 0048 and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Applicant recites a "computer readable medium" in claim 82 however applicant's specification does not provide proper antecedent basis for such claim subject matter.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-

type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969). A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-95 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-60 of copending Application No. 11/137031. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-95 of the current application are envisioned by claims 1-60 of the copending application 11/137031.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 82-95 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Currently, claims 82-95 are drawn to a computer product in a computer readable medium. The term "medium" however under the broadest interpretation includes a transitory signal for which the office considers to be non-statutory subject matter. As such the applicant is advised to include either in the claim language or in the specification subject matter reciting that the medium does not include a signal.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hall in view of Katsikas (WO 01/16695 (cited from IDS)) and further in view of Hardt (US Patent Publication No. 20050114453).

7. As to claim 1, Hall teaches a method for selectively allowing or denying communication access to a recipient user coupled to an electronic communications network by other users, said recipient user having an associated recipient identifier, comprising the steps of:

generating by a security module a plurality of distinct proxy identifiers (i.e., channel id) associated with said recipient user, each of said proxy identifiers (i.e., channel id) having at least three associated security states (i.e., three classes) [col. 6, lines 50-60],

a first of said states being indicative of allowing any other user coupled to said electronic communication network communication access to said recipient user (i.e., Hall teaches a public channel [col. 7, ines 1-5]),

a second of said states being indicative of denying any other user coupled to said electronic communication network communication access to said recipient user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

and a third of said states being conditionally indicative of allowing at least one but fewer than all other user coupled to said electronic communication network communication access to said recipient user if predetermined criteria are met and

denying access to said recipient user otherwise (i.e., Hall teaches a private channel (class for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]);

receiving by a receiver an inbound message from a sender user coupled to said electronic communication network including a sender identifier and said recipient identifier, said sender identifier being associated with the sender user of said inbound message, and said recipient identifier being one of said proxy identifier and transfering (i.e., send) said inbound message to a queue storage (i.e., Hall teaches receiving a message (fig. 6,602). Hall teaches send the message to personal channel agent [fig. 6,612]);

processing by the security module (i.e., strips off the channel id) said transferred inbound message to determine a security status associated therewith pursuant to security settings alterable by said recipient user and using (i.e., Hall teaches the PCA strips off the channel ID from message header information ...Hall teaches a channel class designation for which classifies a sender and recipient communication [col. 6, lines 60- 67]);

allowing communication access for said transferred inbound message to said recipient user when said security status corresponds to said third state and meets one or more of said predetermined criteria (i.e., channel classes) at least partially related to said security status of said one proxy identifier (i.e., channel id), and denying communication access for said transferred inbound message to said recipient user

otherwise (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]).

Hall does not expressly teach:

pursuant to said determination controlling by the queue storage communication access for said transferred inbound message to said recipient user by:

allowing communication access for said transferred inbound message to said recipient user when said security status corresponds to said first state;

denying communication access for said transferred inbound message to said recipient user when said security status corresponds to said second state.

However, the feature of controlling communication access for email communication based on predetermined rules for distinct participating network users is well known in the art and would have been an obvious modification of the system disclosed by Hall as introduced by Katsikas. Katsikas discloses: controlling communication access for said transferred message to said user by (to provide communication access [abstract]): allowing communication access for said transferred message to said user when said security status corresponds to said first state (to provide predetermined rules for controlling message communication between distinct network user [pg. 5, lines 15-25]); denying communication access for said transferred message to said user when said security status corresponds to said second state. Therefore, given the teachings of Katsikas, a person having ordinary skill in the art at the time of the invention would have

recognized the desirability and advantage of modifying Hall by employing the well known feature communication control using predetermine communication rules disclosed above by Katsikas, thereby enhancing the filtering of Spam messages within a network [pg. 10, 19- 30].

The System of Hall in view of Katsikas does not expressly teach determining by a security module pursuant to security settings alterable by said recipient user. However, at the time of applicant's original filing, Hardt disclosed alterable communication settings to determine how to handle message traffic. See Hardt paragraph 45. Therefore, given Hall and Katsikas ability to selectively allow communication access, a person having ordinary skill in the art would have recognize the advantage of modifying Hall to enhance access performance with the feature of dynamic set changing as discussed above by Hardt.

8. As to claim 2, Hall teaches a method where said identifiers are e-mail address and said recipient identifier is an email address (1126, fig. 11).

9. As to claim 3, Hall teaches a system for selectively allowing or denying communication access to recipient user coupled to an electronic communication network by other users coupled to the electronic communications network, said user having an associated recipient identifier, comprising:

a generator for generating a plurality of distinct proxy identifiers (i.e., channel id) associated with said recipient user, each of said proxy identifiers having at least three associated security states (i.e., channel classes 0,1,2), a first of said states being indicative of allowing any other user coupled to said electronic communication network communication access to said recipient user (i.e., Hall teaches a public channel [col. 7, lines 1-5]),

a second of said states being indicative of denying any other user coupled to said network access to said user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

and a third of said states being conditionally indicative of allowing at least one but fewer than all other users coupled to said electronic communication network communication access to said recipient user if predetermined criteria are met and denying access to said recipient user otherwise (i.e., Hall teaches a private channel (class for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]);

a message transferor for receiving an inbound message from a said sender user coupled to said electronic communication network including a sender identifier and said recipient identifier, said sender identifier being associated with the sender user of said inbound message, and transferring (i.e., send) said inbound message to a queue location (i.e., Hall teaches receiving a message (fig. 6,602). Hall teaches send the message to personal channel agent [fig. 6,612]);

said sender identifier and said recipient identifier (col. 11, lines 1-26),

and allowing communication access for said transferred inbound message to said recipient user when said security status corresponds to said third state end meets one or more of said predetermined criteria at least partially related to said security states of said one proxy identifier, and denying communication access for said transferred message to said recipient user otherwise (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]),

Hall does not expressly teach:

pursuant to said determination a gate for controlling communication access for said transferred inbound message to said recipient user by:

allowing communication access for said transferred inbound message to said recipient user when said security status corresponds to said first state;

denying communication access for said transferred inbound message to said recipient user when said security status corresponds to said second state.

However, the feature of controlling communication access for email communication based on predetermined rules for distinct participating network users is well known in the art and would have been an obvious modification of the system disclosed by Hall as introduced by Katsikas. Katsikas discloses: controlling communication access for said transferred message to said user by (to provide communication access [abstract]): allowing communication access for said transferred

message to said user when said security status corresponds to said first state (to provide predetermined rules for controlling message communication between distinct network user [pg. 5, lines 15-25]); denying communication access for said transferred message to said user when said security status corresponds to said second state. Therefore, given the teachings of Katsikas, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hall by employing the well known feature communication control using predetermine communication rules disclosed above by Katsikas, thereby enhancing the filtering of Spam messages within a network [pg. 10, 19- 30].

The System of Hall in view of Katsikas does not expressly teach processing said transferred inbound message to determine a security status associated with said transferred inbound message pursuant to security setting alterable by said recipient user. However, at the time of applicant's original filing, Hardt disclosed alterable communication settings to determine how to handle message traffic. See Hardt paragraph 45. Therefore, given Hall and Katsikas ability to selectively allow communication access, a person having ordinary skill in the art would have recognize the advantage of modifying Hall to enhance access performance with the feature of dynamic set changing as discussed above by Hardt.

10. As to claim 4, Hall teaches a system where said identifiers are e-mail address and said recipient identifier is an e-mail address (1126, fig. 11).

11. As to claim 5, Hall teaches a method where at least one of the generated proxy identifiers (i.e., channel id) associated with said recipient user is substantially absent content that identifies said user (col. 11, lines 28-33).

12. As to claim 6, Hall teaches a method where at least one of the generated proxy identifiers (i.e., channel classes) associated with said recipient user is valid for a predefined time period (i.e., Hall teaches user defined channel class capability [col. 7, lines 10 -20]).

13. As to claim 7, Hall teaches a method where the plurality of proxy identifiers (i.e., channel id) are stored in a database (fig. 11).

14. As to claim 8, Hall teaches a method where an entry in the database includes data representing a contact name associated with said sender user (1118, fig. 11), a proxy identifier assigned to said user (1126, fig. 11), and the security state associated with the proxy identifier (1106, 1108, 1110, fig. 11).

15. As to claim 9, Hall teaches a method where processing said inbound message includes attempting to match (i.e., look up) said recipient identifier with at least one of

the plurality of proxy identifiers (i.e., channel id) associated with said recipient user (i.e., Hall teaches a comparison match for which a channel id is selectively compared among a plurality [col. 11, lines 35-55]).

16. As to claim 10, Hall teaches a method where processing said inbound message includes attempting to match said sender identifier with at least one of a plurality of identifiers (i.e., channel id) associated with contacts of the recipient user (col. 11, lines 40- 53).

17. As to claim 11, Hall teaches a method where processing said inbound message includes determining the security state (i.e., channel classes) associated with said sender user (i.e., Hall teaches channel classes [0,1,2] associated with a correspondents address. Hall teaches the channel classes indicate how sender and recipient are to communicate [col. 11, lines 1-20]).

18. As to claim 12, Hall teaches a method where denying transfer of said message to said recipient user includes sending a reply message to said sender user (606, fig. 6).

19. As to claim 13, Hall teaches a method where denying transfer of said message to said recipient user includes sending a reply message to said sender user (610, fig. fig.6), where said reply message includes one of said plurality of proxy identifiers (i.e., channel id) associated with said recipient user (i.e., Hall teaches evaluating a channel

ID to determine if the channel id exist [608, fig. 6] Hall teaches sending a message to sender [610, fig.6]).

20. As to claim 14, Hall teaches a method where denying (i.e., reject) transfer of said message to said recipient user includes generating a proxy identifier (i.e., channel id) associated with said recipient user and sending a reply message to said sender user (i.e., Hall teaches sending a "no permission message" to sender for which said sender is associated with a channel id [1126, fig. 11]), where said reply message (i.e., "no permission message" [610, fig. 6]) includes the generated proxy identifier (i.e., channel id) associated with said recipient user [fig. 11].

21. As to claim 15, Hall teaches a method where denying (i.e., no correspondent key entry) transfer of said message to said recipient user includes entering said sender identifier into a database (i.e., UCDB) (col. 10, lines 55-67).

22. As to claim 16, Hall teaches a method where allowing transfer of said message to said recipient user includes determining if said recipient user replied to a message previously sent from said sender user(i.e., Hall teaches a correspondent address associated with channel id [fig. 4] Hall teaches a correspondent known to the recipient (i.e., received email from correspondent previously)will have a channel id [col. 12, lines 15-25]).

23. As to claim 17, Hall teaches a method where allowing transfer of said message to said recipient user includes determining if said recipient user initiated generation of a proxy identifier included in the message (i.e., Hall teaches determining if known user [606, fig. 6] Hall further teaches determining if channel id exist [col. 12, lines 15-25]).

24. As to claim 18, Hall teaches a method where said user-generated proxy identifier absent (i.e., unknown user) from said plurality of proxy identifiers (col. 12, lines 15-25).

25. As to claim 19, Hall teaches a method further comprising the step: if said user-generated proxy identifier is absent from said plurality of proxy identifiers, adding (i.e., enter) said user generated proxy identifier to said plurality of proxy identifiers (i.e., Hall teaches determining if this a first-time sender. Hall teaches the action to capture correspondent information [col. 12, lines 55-65]).

26. As to claim 20, Hall teaches a method where allowing transfer of said message to said recipient user includes removing (i.e., strip off) reference to said user- generated proxy identifier in said message (col. 12, lines 35-40).

27. As to claim 21, Hall teaches a method where allowing transfer of said message to said recipient user includes removing (i.e., strip off) reference to said user-generated proxy identifier in said message and adding an e-mail address associated with said recipient user to said message (col. 12, lines 35-40).

28. As to claim 22, Hall teaches a method where processing said inbound message includes removing (i.e., separate) reference to said recipient identifier (i.e., channel id)included in said message (i.e., Hall teaches processing a message involves employing a process of separation [col. 11, lines 40-45]).

29. As to claim 23, Hall teaches a method where said first state that is indicative of allowing any other user coupled to said electronic communication network communication access to said recipient user, includes allowing transfer of a message from said other user to said user (i.e., Hall teaches a public channel [col. 7, lines 1-5]).

30. As to claim 24, Hall teaches a method where said second state that is indicative of denying any other users coupled to said electronic communication network communication access to said recipient user, includes blocking transfer of a message from said any other coupled to said user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]).

31. As to claim 25, Hall teaches a method where said predetermined criteria includes the user previously responding to a message previously sent by the sender (i.e., Hall teaches a correspondent address associated with channel id [fig. 4] Hall teaches a correspondent known to the recipient (i.e., received email from correspondent previously)will have a channel id [col. 12, lines 15-25]).

32. As to claim 26, Hall teaches a method where said previously sent message includes said sender identifier (i.e., key) (i.e., Hall teaches a previous message sent by sender containing a key for which could be used to determine the sender to be legitimate [col. 15, lines 15-25]).

33. As to claim 27, Hall teaches a method where one of the predetermined criteria includes the sender identifier (i.e., key) matching (i.e., locating) one of a plurality of identifiers (i.e., Hall teaches locating key in UCDB [col. 15, lines 25- 35]).

34. As to claim 29, Hall teaches a method where one of the predetermined criteria includes the recipient identifier matching one of the plurality of proxy identifiers (i.e., Hall teaches a comparison match for which a channel id is selectively compared among a plurality [col. 11, lines 35-55]).

35. As to claim 30, Hall teaches a method where one of the predetermined criteria includes both the recipient identifier and the sender identifier are associated with the same network domain (i.e., host) (i.e., Hall teaches a channelized address specifying a host name (i.e., domain name) [col. 5, lines 45- 50; 200, fig. 3]).

36. Claims 31-95 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hall in view of Hardt.

2. As to claims 31 and 68, Hall teaches a method for selectively allowing or denying communication access to a recipient user coupled to an electronic communication network by other users coupled to the electronic communications network, comprising the steps of:

receiving by a receiver an inbound message over the electronic communications network from a sender user [fig. 2], where the inbound message includes a sender identifier associated with a sender user and an recipient identifier associated with the recipient user [1118, 1126, fig. 11];

and using said sender identifier and recipient identifier one of at least three security states associated with the inbound message (col. 11, lines 1-26),

where a first security state is indicative of allowing delivery of the inbound message to the recipient user (i.e., Hall teaches a public channel [col. 7, lines 1-5]),

a second security state is indicative of denying delivery of the inbound message to the recipient user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

a third security state is indicative of conditionally allowing delivery of the message to the recipient user (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]), each of the at least three security states (i.e., channel classes) are associated with the sender identifier and the recipient identifier included in the inbound message (i.e., Hall teaches channel classes associated with a sender and receiver [col. 11, lines 1-21]).

Hall does not expressly teach and determining by a security module pursuant to security settings alterable by said recipient user. However, at the time of applicant's original filing, Hardt disclosed alterable communication settings to determine how to handle message traffic. See Hardt paragraph 45. Therefore, given Hall ability to selectively allow communication access, a person having ordinary skill in the art would have recognize the advantage of modifying Hall to enhance access performance with the feature of dynamic set changing as discussed above by Hardt.

3. As to claim 32, Hall teaches a method where determining one of the at least three security states (i.e., channel classes) includes determining (i.e., look up) if the recipient identifier matches one of a plurality of proxy identifiers (i.e., Hall teaches a channel id comparison among a plural channel ids contained in a file [col. 11, lines 45-50]).

4. As to claim 33, Hall teaches a method further comprising: prior to delivery, replacing each reference to the recipient identifier in the message with an identifier associated with the user if the recipient identifier matches one of a plurality \of proxy identifiers [fig. 10C, fig. 10D, fig. 10E].

5. As to claim 34, Hall teaches a method where determining one of the at least three security states (i.e., channel classes) includes determining if the sender identifier matches one of a plurality of sender identifiers (col. 11, lines 35- 45).

6. As to claim 35, Hall teaches a method where the recipient identifier is a proxy identifier (i.e., channel id) that is substantially absent content that identifies said recipient user (col. 12, lines 10-25).

7. As to claim 36, Hall teaches a method where the identifiers are e-mail addresses (1126, fig. 11).

8. As to claim 37, Hall teaches a method where detecting the second security state (i.e., channel class 0) initiates sending a reply message to the sender user to report the delivery denial (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60- 62]) Hall teaches sending a "No Permission" message [610, fig. 6]).

9. As to claim 38, Hall teaches a method where detecting the second security state initiates (i.e., channel class 0) sending a reply message to the sender user that reports the delivery denial (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62] Hall teaches sending a "No Permission"

message [610, fig. 6]), where the reply message includes a proxy identifier associated with the recipient user for sending a future message [610, fig. 6].

10. As to claim 39, Hall teaches a method where detecting the third security state associates an alert indicator (i.e., channel class 1) with the message (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67; col .11, lines 1-6]).

11. As to claim 40, Hall teaches a method where the alert indicator includes a flag (i.e., channel classes [0,1,2]) that is associated with the inbound message (col. 11, lines 1-21).

12. A to claim 41, Hall teaches a method where the third security state is triggered if the inbound message is a response to a message previously sent by the recipient user to the sender [col. 11, lines 1-5].

13. As to claim 42, Hall teaches a method where the third security state is triggered if the recipient identifier included in the inbound message is a proxy identifier (i.e., channel id) generated by the user and is absent from the plurality of proxy identifiers (i.e., Hall teaches a private channel (class 1) for which a recipient user expect one or a limited number on that particular channel [col. 6, lines 65-67]).

14. As to claim 43, Hall teaches a method where the third security state is triggered if the recipient identifier and the sender identifier include the same network domain (i.e., host) (i.e., Hall teaches a channelized address specifying a host name (i.e., domain name) [col. 5, lines 45-50; 200, fig. 3]).

15. As to claim 44, Hall teaches a method where the recipient identifier (i.e., channel classes) is a proxy identifier assigned to the sender user for a period of time (i.e., Hall teaches user defined channel class capability [col. 7, lines 10 -20]).

16. As to claim 45, Hall teaches a system where at least one of the generated proxy identifiers (i.e., channel id) associated with said recipient user is substantially absent content that identifies said recipient user (col. 12, lines 15-25]).

17. As to claim 46, Hall teaches a system where at least one of the generated proxy Identifiers (i.e., channel classes) associated with said sender user is valid for a predefined time period (i.e., Hall teaches user defined channel class capability [col. 7, lines 10 -20]).

18. As to claim 47, Hall teaches a system further comprising: a database (i.e., UCDB) configured to store the plurality of proxy identifiers (col. 10, lines 55-67).

19. As to claim 48, Hall teaches a system the database (i.e., UCDB) includes an entry that stores data that represents a contact name associated with said sender user, a proxy identifier assigned to said sender user, and the security state associated with the proxy address (col. 10, lines 55-67).

20. As to claim 49, Hall teaches a system where the processor attempts to match said sender identifier with a least one of a plurality of identifiers associated with the recipient user (col. 12, lines 15-25).

21. As to claim 50, Hall teaches a system where the processor determines the security state (i.e., channel classes) associated with said sender user that overrides the security state associated with the message [col. 7, lines 10-30].

22. As to claim 51, Hall teaches a system where the processor determines if said recipient identifier matches one of said plurality of proxy identifiers associated with said recipient user (608, fig. 6).

23. As to claim 52, Hall teaches a system where the gate initiates sending a reply message to said sender to report denying (i.e., reject) transfer of said inbound message (610, fig. 6).

24. As to claim 53, Hall teaches a system where the gate initiates sending a reply message to said sender user to report denying transfer of said inbound message, wherein said reply message (i.e. "No permission") includes one of said plurality of proxy identifiers associated with said recipient user (610, fig. 6).

25. As to claim 54, Hall teaches a system where the processor initiates entering said sender identifier into a database (i.e., UCDB) when access to the recipient user by transferring said inbound message is denied (col. 10, lines 55-67).

26. As to claim 55, Hall teaches a system where the processor determines if said recipient user replied to a previously sent message from said sender to determine whether to transfer said inbound message to said recipient user (i.e., Hall teaches a correspondent address associated with channel id [fig. 4] Hall teaches a correspondent known to the recipient user (i.e., received email from correspondent previously) will have a channel id [col. 12, lines 15-25]).

27. As to claim 56, Hall teaches a system where the processor determines if said recipient user initiated generation (i.e. known user) of said recipient identifier to determine whether to transfer said message to said recipient user [604,606, fig. 6].

28. As to claim 57, Hall teaches a system where said user-generated recipient identifier (i.e., channel id) is absent from said plurality of proxy identifiers [609, fig. 6].

29. As to claim 58, Hall teaches a system where if said processor determines that said user-generated recipient identifier is absent, said processor initiates adding said user-generated recipient identifier into said plurality of proxy identifiers (i.e., Hall teaches a first message to recipient [col. 12, lines 55-67]).

30. As to claim 59, Hall teaches a system where if said inbound message is transferred to said recipient user, said processor initiates removing (i.e., strip off) from any reference to said recipient identifier from said message (col. 12, lines 35-40).

31. As to claim 60, Hall teaches a system where if said inbound message is transferred to said user, said processor initiates adding a reference to an identifier associated with the recipient user in said transferred inbound message (fig. 10C, fig. 10D, fig. 10E).

32. As to claim 61, Hall teaches a system where if said first security state is detected (i.e., Hall teaches a public channel [col. 7, lines 1-5]), the gate allows transfer of said inbound message to said recipient user (col. 12, lines 22-25).

33. As to claim 62, Hall teaches a system where if said second state is detected, the gate blocks transfer of said inbound message to said recipient user (i.e., Hall teaches

send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]).

34. As to claim 63, Hall teaches a system where said predetermined criteria includes the recipient user responding to a previously sent message from said sender user (i.e., Hall teaches a correspondent address associated with channel id [fig. 4] Hall teaches a correspondent known to the recipient (i.e., received email from correspondent previously)will have a channel id [col. 12, lines 15-25]).

35. As to claim 64, Hall teaches a system where said previously sent message includes the sender identifier (col. 12, lines 15-25).

36. As to claim 65, Hall teaches a system where the predetermined criteria includes the processor matching the sender identifier to one of a plurality of identifiers (fig. 4).

37. As to claim 66, Hall teaches a system where the predetermined criteria includes the processor matching the recipient identifier to one of the plurality of proxy Identifiers (col. 12, lines 15-20).

38. As to claim 67, Hall teaches a system where the predetermined criteria includes the processor determining that the recipient identifier and the sender identifier are

associated with the same network domain (i.e.host) (i.e., Hall teaches a channelized address specifying a host name (i.e., domain name) [col. 5, lines 45-50; 200, fig. 3]).

39. As to claim 69, Hall teaches a system where the processor determines if the recipient identifier matches one of a plurality of proxy identifiers to determine one of the at least three security states (i.e., Hall teaches checking channel id exist in recipient file [col. 12, lines 15-20] Hall teaches channel classes [0,1 ,.2] representative of how the mail will be treated [col. 6, lines 50-67]).

40. As to claim 70, Hall teaches a system where prior to delivery, the processor is configured to replace each reference to the recipient identifier in the inbound message with an identifier of the recipient user if the recipient identifier matches one of a plurality of proxy identifiers (fig. 10C, fig. 10D, fig. 10E).

41. As to claim 71, Hall teaches a system where the processor is configured to determine if the sender identifier (i.e., key) matches (i.e., locating) one of a plurality of sender identifiers (i.e., Hall teaches locating key in UCDB [col. 15, lines 25-35]).

42. As to claim 72, Hall teaches a system where the recipient identifier is a proxy identifier (i.e., channel id) that is substantially absent content that identifies said recipient user (col. 11, lines 28-33).

43. As to claim 73, Hall teaches a system where the sender identifier is an e- mail address and the recipient identifier is an email address (1126, fig. 11).

44. As to claim 74, Hall teaches a system where when the second security state is detected, the processor initiates sending a reply message to the sender user to report the delivery denial (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62] Hall teaches sending a "No Permission" message [610, fig. 6]).

45. As to claim 75, Hall teaches a system where when the second security state is detected, the processor initiates sending a reply message to the sender user to report the delivery denial, where the reply message includes a proxy identifier to send a future message (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62] Hall teaches sending a "No Permission" message [610, fig. 6]).

46. As to claim 76, Hall teaches a system where when the third security state is detected, an alert indicator is associated (i.e., channel class 1) with the message (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67;col .11, lines 1-6]).

47. As to claim 77, Hall teaches a system where the alert indicator includes a flag (i.e., channel class designation [0,1,2]) that is associated with the inbound message (col. 11, lines 1-20).

48. As to claim 78, Hall teaches a system where the third security state is triggered if the message is a response to a previously sent message from the recipient user to the sender (i.e., Hall teaches a private channel (class 1) for which a recipient user expect one or a limited number on that particular channel [col. 11, lines 1-5]).

49. As to claim 79, Hall teaches a system where the third security state is triggered if the recipient identifier is a proxy identifier generated by the user and is absent from a plurality of proxy identifiers associated with the user that are stored in a database (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65- 67]).

50. As to claim 80, Hall teaches a system where the third security state is triggered (i.e., public channel/channel class 2) if the recipient user identifier and the sender identifier include the same network domain (e.g., anyone can send email) (i.e., Hall teaches any one of a number of correspondents may send e-mail using the public channel ID [col. 11, lines 10-15]).

51. As to claim 81, Hall teaches a system where the recipient identifier is assigned to the recipient user for a period of time (i.e., Hall teaches user defined channel class capability [col. 7, lines 10-20]).

52. As to claim 82, Hall teaches a computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by a processor, cause that processor to:

receive an inbound message to a recipient user over a electronic communications network from a sender user [fig. 2], where the inbound message includes a sender identifier associated with a sender user and an recipient identifier associated with the recipient user [1118, 1126, fig. 11];

transfer said inbound message to a queue storage [fig. 1];

and using said sender identifier and recipient identifier one of at least three security states (i.e., channel classes) associated with the inbound message (col. 5, lines 50-67),

where a first security state is indicative of allowing delivery of the inbound message to the recipient user (i.e., Hall teaches a public channel [col. 7, lines 1-5]),

a second security state is indicative of denying delivery of the inbound message to the recipient user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

a third security state is indicative of conditionally allowing delivery of the message to the recipient user (i.e., Hall teaches a private channel (class 1) for which a

user expect one or a limited number on that particular channel [col. 6, lines 65-67]), each of the at least three security states (i.e., channel classes) are associated with the sender identifier and the recipient identifier included in the inbound message (i.e., Hall teaches channel classes associated with a sender and receiver [col. 11, lines 1-21]).

Hall does not expressly teach and determining by a security module pursuant to security settings alterable by said recipient user. However, at the time of applicant's original filing, Hardt disclosed alterable communication settings to determine how to handle message traffic. See Hardt paragraph 45. Therefore, given Hall ability to selectively allow communication access, a person having ordinary skill in the art would have recognize the advantage of modifying Hall to enhance access performance with the feature of dynamic set changing as discussed above by Hardt.

53. As to claim 83, Hall teaches a computer program product where to determine one of the at least three security states (i.e., channel classes) includes determining if the recipient identifier matches one of a plurality of proxy identifiers (i.e., Hall teaches a channel id comparison among a plural channel ids contained in a file [col. 11, lines 45-50]).

54. As to claim 84, Hall teaches a a computer program product further comprising instruction for: prior to delivery, if the recipient identifier matches one of a plurality of proxy identifiers, replacing each reference to the recipient identifier in the message with

an identifier associated with the user if the recipient identifier matches one of a plurality \of proxy identifiers [fig. 10C, fig. 10D, fig. 10E].

55. As to claim 85, Hall teaches a computer program product where to determine one of the at least three security states (i.e., channel classes) includes determining if the sender identifier matches one of a plurality of sender identifiers (i.e., Hall teaches a channel id comparison among a plural channel ids contained in a file [col. 11, lines 45-50]).

56. As to claim 86, Hall teaches a computer program product where the recipient identifier (i.e., channel id) is a proxy identifier that is substantially absent content that identifies said user (col. 12, lines 10-25).

57. As to claim 87, Hall teaches a computer program product where the sender identifier is an e-mail address and the recipient identifier is an e-mail address (1126, fig. 11).

58. As to claim 88, Hall teaches a computer program product further comprising instructions for: upon detecting the second security state (i.e., channel class 0) (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]), sending a reply message to the sender user to report delivery denial (i.e., Hall teaches sending a "No Permission" message [610, fig. 6]).

59. As to claim 89, Hall teaches a computer program product further comprising instructions for: upon detecting the second security state (i.e., channel class 0) (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]), sending a reply message to the sender that reports the delivery denial (i.e., Hall teaches sending a "No Permission" message [610, fig. 6]), wherein the reply message includes a proxy address to send a future message.

60. As to claim 90, Hall teaches a computer program product further comprising instructions for: upon detecting the third security state (i.e. user expect one or a limited number), associating an alert indicator (i.e., channel class 1) with the inbound message (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 11, lines 1- 20]).

61. As to claim 91, Hall teaches a computer program product where the alert indicator (i.e., channel class designation [0, 1,2]) includes a flag that is associated with the inbound message (col. 11, lines 1-20).

62. As to claim 92, Hall teaches a computer program product where the third security state is triggered if the message is a response to a previously sent message from the recipient user to the sender user [col. 11, lines 1-5].

63. As to claim 93, Hall teaches a computer program where the third security state (i.e., public channel/channel class 2) is triggered if the recipient identifier in the message is a proxy identifier generated by the recipient user and is absent (i.e., use of public channel ID) from a plurality of proxy identifiers that are associated with the recipient user and stored in a database (i.e., Hall teaches any one of a number of correspondents may send e-mail using the public channel ID [col. 11, lines 10- 15] Hall teaches use of public channel ID. Hall teaches correspondents information (i.e., address, channel)in database).

64. As to claim 94, Hall teaches a computer program where the third security state (i.e., public channel/channel class 2) is triggered if the recipient identifier and the sender identifier include the same network domain (e.g., anyone can send email) (i.e., Hall teaches any one of a number of correspondents may send e-mail using the public channel ID [col. 11, lines 10-15]).

65. As to claim 95, Hall teaches a computer program product where the recipient identifier (i.e., channel classes) is assigned to the user for a period of time (i.e., Hall teaches recipient user defined channel class capability [col. 7, lines 10 - 25]).

Response to Arguments

Examiner Remarks – 102(e) & 103(a)

Applicant argues:

> "Hall does not provide a proper basis for either of the outstanding rejections. More particularly, Hall discloses a static security system/method whereby once a communication link between parties has been established; a fixed security aspect exists with respect to that link. As a consequence, in order to change the security aspect/level associated with the linked parties, a new link is required to be established. In contrast, the applicants disclose and claim a dynamic security/method/computer program, whereby once a communication link between parties has been established, including at least one sender user and a recipient user, the recipient user has the ability to change the security settings defining the security aspect/level for that established link, without the need to establish a new link. This cannot be accomplished by the system/method taught or suggested by Hall. Thus, the dynamic security feature of the applicants' invention and claims is materially different from Hall's disclosed or suggested static security system/method. All of the independent claims of the subject application, claims 1, 3, 31, 68 and 82, have now been amended to reflect the dynamic security feature of the applicants' invention and the components of the applicants' invention as claimed (e.g., queue storage, receiver, processor, security module, gate, message transferor, generator). More particularly, the claims all now require a determination of a security status for an inbound message, made pursuant to security settings which are alterable by the recipient user, and using the sender identifier and the recipient identifier".

The Examiner contends applicant's remarks regarding Hall is deficient in teaching a dynamic alterable setting is moot of the new rejection outlined aboved. The new rejection under Hall in view of the teaching of Hardt cures the alleged deficiency. Specifically, Hardt allows for the capability to dynamically manage alias address and communication rules. The alias address conforms to specific communication rules (e.g., security rules). The user maintains the capability to change the alias addresses and rule as so desired. See Hardt paragraph 45.

Applicant further argues:

> "There is no teaching or suggestion in Hall of a dynamic security system/method or the components as defined in each of the independent claims. Instead, Hall teaches a static security system/method, using an "unguessable" channel

> identifier as a part of an address for defining the link and "... for verifying that the message is authorized for delivery to the recipient..."; see Hall at col 3, lines 54-62. Thus, Hall's sender address and recipient address define the link and the security level, since the security level, defined by the unguessable channel identifier, is a portion of the address. If Hall wishes to change the security level associated with a link between two parties on his system or using his method, he cannot change the security level without changing the address, since the link is defined by the address. Therefore, Hall must open another link, characterized by a different "unguessable" channel identifier, to change the security level linking the two parties. In contrast, the systems and methods defined by applicants' independent claims, permit an established link to be used while the recipient user can adjust the security aspects of the link dynamically, without requiring a new link to be established".

Again the Examiner asserts Hall in view of Hardt allows for the dynamic changing of communication settings and dynamic rules (e.g., security rules) associated with said communicating setting. Refer to rejection above.

With regards to applicant's statement of:

> "Katsikas discloses a system for eliminating unauthorized email sent to a user using an "authorized senders" list (ASL list); Katsikas, abstract. There is no teaching or suggestion in Katsikas of a dynamic security system/method or the components as defined in each of the independent claims. Instead, Katsikas describes eliminating unwanted email based on the sender address using the ASL; Katsikas, page 1, lines 7-8. Accordingly, Katsikas does not cure the deficiencies in the teachings by Hall. It is submitted that all of the independent claims of the subject application, claims 1, 3, 31, 68 and 82, and claims 2, 4-30, 32-67, 69-81, and 83-95 dependent thereon, now fully and clearly define the dynamic security features of the applicants' invention, and that the claimed system/method/computer program for allowing or dewing communication access, are patentably distinct over Hall alone, or in combination with Katsikas".

The Examiner contends that the combination of Hall, Katsikas and Hardt allows for dynamic changing of communication parameters. Specifically, Hardt allows for

associating communication rules to alias address. Additionally, Hardt allows for dynamic management of the communication rules and alias address. See Hardt paragraph 45.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431